

INFORMATION BULLETIN

JOB TRAINING PARTNERSHIP ACT

Number: B98-109

Date: June 21, 1999
Expiration Date: 06/30/00
69:47:jws:2935

TO: SERVICE DELIVERY AREA ADMINISTRATORS
PRIVATE INDUSTRY COUNCIL CHAIRPERSONS
JTPD PROGRAM OPERATORS
EDD JOB SERVICE OFFICE MANAGERS
JTPD STAFF

SUBJECT: BUSINESS CONTINUITY AND CONTINGENCY PLAN FOR YEAR 2000

The Department of Labor (DOL) issued Training and Employment Notice (TEIN) 19-98, to provide additional Year 2000 (Y2K) Guidance to the Job Training Partnership Act (JTPA) State system. This will ensure that its mission critical systems can provide services to participants in the event of disruption in services caused by Y2K or other infrastructure failures. As such, DOL requests that the states forward TEIN 19-98 to their Service Delivery Areas (SDA). Additionally, DOL asks the SDAs to voluntarily complete a Business Continuity and Contingency Plan (BCCP). Finally, DOL expects the states to oversee this action and report the results to the Regional Offices.

Therefore, the State of California asks that the SDAs complete the Working Table—Risk Assessment Steps. The table is located on the last page of the JTPA BCCP "Self Assessment Guide" which is attached to TEIN 19-98. Please submit the completed Risk Assessment on August 10, 1999, and November 10, 1999.

For your convenience the Self Assessment Guide is available in Microsoft Word 97. The form can be accessed on the Job Training Partnership Division web site in the Resource Information Center under Miscellaneous Forms. The completed document can be e-mailed to: JTPDLIB@EDD.CA.GOV (please include BCCP in the subject line). The document can also be sent to the following address:

The JTPD-BCCP Desk
P.O. Box 826880, MIC 69
Sacramento, CA 94280-0001

If you have any questions, please direct them to Jim Scholl at (916) 657-4610.

/S/ BILL BURKE
Assistant Deputy Director

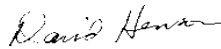
Attachment

<p align="center">U. S. Department of Labor Employment and Training Administration Washington, D.C. 20210</p>	CLASSIFICATION Y2K
	CORRESPONDENCE SYMBOL TD
	DATE February 9, 1999

TRAINING AND EMPLOYMENT INFORMATION NOTICE NO. 19-98

TO: ALL STATE JTPA LIAISONS
ALL STATE EMPLOYMENT SECURITY AGENCIES
ALL ONE-STOP CAREER CENTER SYSTEM LEADS
ALL STATE WORKER ADJUSTMENT LIAISONS

FROM: DAVID HENSON
Director
Office of Regional



SUBJECT: Year 2000 Business Continuity and
Contingency Planning (BCCP) for JTPA System

1. **Purpose.** To provide additional Year 2000 Guidance (Y2K) to the JTPA State system to ensure that its mission critical systems can provide services to participants in the event of disruption in services caused by Y2K or other infrastructure failures.
2. **References.** TEGL 7-97; GAO Year 2000 Computing Crisis: Business Continuity and Contingency Planning, (Aug. 1998). E-mail address: <<http://www.gao.gov/special.pubs/bcguide.pdf>>.
3. **Background.** The Department's Y2K policy is to ensure that federally funded employment and training programs provide services to eligible participants through the millennium. ETA has addressed this policy over the past 18 months by providing Y2K technical guidance, information via Web sites, mini-assessments, and workshops. However, as the Year 2000 fast approaches, proactive management requires that States anticipate, that in spite of their efforts to address Y2K readiness, some potential remains for program disruption.
4. **Findings** As a result of the JTPA mini-assessment, the San Francisco and Denver workshops, and, ITSC's (contractor) risk analysis, some States/SDA's appear to be "at risk" in the areas of eligibility determination, reporting, and financial vendor payments. These problems could seriously affect operations. To address these

RESCISSIONS	EXPIRATION DATE Continuing
--------------------	--------------------------------------

problems and meet the “due diligence” legal test, State agencies would be prudent to have a “business continuity and contingency plan” (BCCP), which identifies core agency functions, defines future failure scenarios, and outlines alternative processes that would be followed in the event of a Year 2000 problem or infrastructure failure in power or communication.

5. **Proposal** ETA believes that “risk assessment, business continuity, and contingency planning” is the most appropriate strategy for State agency management at this time. Thus, ETA is providing States/SDAs with a GAO model “Business Continuity Planning Structure,” composed of a) *Initiation*, b) *Business Impact Analysis*, c) *Contingency Planning*, and d) *Testing*.

The first phase, *Initiation*, consists of establishing a State/SDA workgroup of high level management to address strategy, schedules and support.

The second phase, *Business Impact Analysis* consists of assessing the potential impact of mission critical system failures versus the agency’s core business. ETA is providing a format, Attachment I, which enables the agency’s managers to self assess the Y2K readiness relative to the risk of operational failure for their program. If the management determines the self-assessment instrument yields a high-risk score, it would suggest the State develop a fail-safe contingency plan.

The third phase, *Contingency Planning* consists of identifying and documenting plans, triggers, and business resumption for each core business process.

The final phase, *Testing* determines if the plan really works.

The next steps are developing periodic updates, and making sure staff know the plans, the triggers, and their responsibilities. In addition, ETA’s Y2K contractor, ITSC, will be available for technical guidance via teleconference on a scheduled basis for the period February 17 through May 1999. ITSC also has a web page at <www.itsc.state.md.us> which lists guidance on these and other relevant employment and training Y2K topics. The Social Security Administration’s (SSA) “BCCP” has useful formats covering “risk, timing, priority, strategy, responsible unit, and contingency triggers.”

This concept was discussed and determined feasible by a group of ETA Regional and State staff at the Denver MIS conference in early December 1998.

The concept would provide State agency management with the tools to better assess risk, develop appropriate BCCPs, and ensure program continuity for mission critical business functions. The voluntary nature supports the partnership roles defined in TEGL 7-97, and reinforces State responsibility for program continuity. ETA believes that the process is important, however, the “suggested formats” are optional.

6. **Action Required.** JTPA liaisons are requested to 1) Distribute the voluntary BCCP materials to State/SDA management and request they begin the process as soon as possible; 2) Track State/SDA's progress in completing the process and BCCP products; and 3) Inform the respective Regional Office's designated Y2K contact person, periodically, of the status.

7. **Attachments**

- I. JTPA BCCP "Self Assessment Guide"
- II. GAO's "Year 2000 Computing Crisis: Business Continuity and Contingency Planning (<http://www.gao.gov/special.pubs/bcpguide.pdf>)
- III. [SSA's "Business Continuity and Contingency Plan"](#) Version 4, Dec. 31, 1998

JTPA Year 2000 (Y2K) Self-Assessment Instrument

For the State of California, SDA _____

Overview

The purpose of this Y2K Self-assessment guide is to allow the JTPA technical manager to assess the status of their Y2K readiness and response relative to the risk of operational failure that their organization may experience. The assessment requires that the manager identify their major business functions, categorize their importance and evaluate specific Y2K risks those systems may experience. By following the steps of the self-assessment instrument, the user can determine the type of contingency plan(s) that are required to provide adequate protection and back up from operational failures associated with Y2K system errors or operational cessation.

Step 1: Identify Business Functions

The JTPA manager must review their operations and lay out the major JTPA operations that are supported by some level of computer systems automation. Typical functions can include for example: pay vendor invoices; provide SPIR, financial reporting data; exchange data with other agencies; and provide services to clients.

Each business function is categorized as **(1) mission critical; (2) supports operations; (3) ancillary**.

1. **A mission critical business** function can be described as an operational activity that is necessary for the day to day functioning of the enterprise. Without this business function the enterprise is unable to perform their mission. The impact of failure is immediate (1 week or less) and substantial monetary penalties may result from the failure of this business function.
2. **A business function that supports the operations** can be described as an operational activity that is necessary for long term operations but workloads or non-performance is possible for less than 30 days. Some monetary penalties may result from the failure of this business function.
3. **An ancillary business function** may be equated with an amenity. The feature adds value to the operations but most likely does not result in an ability to perform the core mission or accrue monetary penalties.

	<u>Business Function</u>	<u>Category</u>
Examples	Pay vendor invoices	2
	Participate tracking	1
	Provide SPIR reporting data	2
	Exchange data with another agency	2
	Provide 1 on1 counseling services with clients	1
	E-mail	2
	Voice mail	3
	General office software (Word processing, Spreadsheets, standalone database products etc.)	2
	Provide internet access for client training	3

Step 2: Perform a Risk Assessment of Each Business Function:

The JTPA manager must next perform a risk assessment for each business function in a series of categories related to the activities necessary to fix and test automation systems in preparation for Y2K error free operation. The areas or rating relate to: (A) if the repair, remediation, or replacement of the system will be performed on time, (B) whether adequate testing of the repaired or replaced system will be performed, (C) the risks the JTPA operation faces from other organizations with which it exchanges data and information, (D) whether the JTPA agency has adequate IT resources available to respond to Y2K errors as they occur when critical calendar dates are reached, and (E) availability of support from active hardware and software vendors for the hardware and software being used.

Risk assessment factors and rating:

Item A – Remediation, Repair, and Replacement Schedule

10 --	Remediation of Hardware, Software and Data <i>will not be completed</i> by Y2K drop dead date.
7 --	Remediation of Hardware, Software and Data <i>will be completed</i> 60 days before Y2K drop dead date.
3 --	Remediation of Hardware, Software and Data <i>will be completed</i> 120 days before Y2K drop dead date.
1 --	Remediation of Hardware, Software and Data <i>will be completed</i> 180 days before Y2K drop dead date.

Item B – Systems Y2K Testing

10 --	Remediated Hardware, Software and Data <i>was not or will not</i> be future date tested.
3 --	Remediated Hardware, Software and Data <i>was tested or will be tested</i> with the current date, a roll over scenario and various year 2000 dates including Feb. 29, 2000.
1 --	Remediated Hardware, Software and Data <i>was or will be</i> verified by an independent resource.

Item C – Y2K Status of Data Exchange Partners

10 --	Vendors or other agencies that you exchange data with <i>are not expected</i> to Y2K ready to receive or send you data by the Y2K drop dead date.
7 --	Vendors or other agencies that you exchange data with <i>are expected</i> to Y2K ready to receive or send you data 60 days before the Y2K drop dead date.
3 --	Vendors or other agencies that you exchange data with <i>are expected to be</i> Y2K ready to receive or send you data 120 days before the Y2K drop dead date.
1 --	Vendors or other agencies that you exchange data with <i>are expected</i> to Y2K ready to receive or send you data 180 days before the Y2K drop dead date.

Item D – JTPA Agency Y2K IT Capabilities

10 --	Minimal agency system support staff <i>are available</i> to help diagnose and correct Y2K Hardware and Software problems.
7 --	Agency system support staff <i>are unfamiliar</i> with agency Hardware and Software but agency talent exists to help diagnose and correct Y2K problems.
1 --	Agency system support staff are familiar with and ready to support Hardware, Software, or data that develops Y2K bugs.

Item E – Y2K Hardware and Software Vendor Support

10 --	Application vendors that developed software <i>are no longer</i> in business.
1 --	Application vendors (Maintenance contracts are in place) <i>are familiar with</i> and ready to support Hardware, Software, or data that develops Y2K bugs.

Notes:

Hardware should include items such as computers (PC's, Unix boxes, Mainframes), and network devices such as routers.

Software should include items such as operating systems, database software, application software, development software, network software, and server software such as WEB servers and specialty servers such as an SNA gateway server.

Some items may be N/A for a particular business function:

Step 3: Assemble a Risk Assessment Table

Each business function is rated for each Y2K item. Business functions that are categorized as mission critical (1) are high risk and assigned a multiplier factor of 1. Business functions that support operations (2) are moderate risk and are assigned a multiplier factor of .8. ancillary business functions are low risk and are assigned a multiplier factor of .4. The item number with the highest risk factor is multiplied by the multiplier factor to arrive at the risk assessment rating.

Example:

Business Function	Cat.	Risk Group/ Multiplier	Item A	Item B	Item C	Item D	Item E	Risk Rating
Pay vendor invoices	2	Mod / .8	7	3	7	1	1	5.6
Participant tracking	1	High / 1.0	10	10	N/A	7	10	10
Provide SPIR reporting data	2	Mod / .8	3	3	3	1	N/A	2.4
Exchange data with another agency	2	Mod / .8	10	10	10	10	10	8.0
Provide 1 on 1 client counseling services	1	High / 1.0	N/A	N/A	N/A	N/A	N/A	0
General office e-mail	2	Mod / .8	3	3	3	1	1	2.4
General office voice mail	3	Low / .4	1	1	N/A	N/A	1	.4
Office suite software	2	Mod / .8	3	3	3	1	1	2.4
Internet access for client training	3	Low / .4	7	3	N/A	7	1	2.8

Interpretation: Business functions that have a Risk Assessment Rating in the top third (roughly 7.0 or higher) should be considered a high-risk business function. A contingency plan for those business functions should consider a risk mitigation strategy that includes items such as additional resources to complete the Y2K remediation, fully test etc.--if this is possible--or the development of a contingency system that would provide a fail safe fallback to perform the business function until the system is Y2K compliant.

A business function that has a Risk Assessment Rating in the middle third (roughly 4 to 6.9) should have a contingency plan and contingency solution identified. The remediation progress should be closely monitored to determine if the contingency solution needs to be developed or implemented.

Business functions that fall into the bottom third (roughly below 4) of the Risk Assessment Rating should have their progress monitored and a preliminary contingency plan developed.

Working Table

Risk Assessment Steps:

1. Identify additional business functions and write the descriptions in column 1.
2. Rate the business functions as a category 1, 2, or 3 and assign the corresponding risk group multiplier. Category 1 business functions are in the high-risk group with a multiplier of 1. Category 2 business functions are in the moderate-risk group with a multiplier of .8. Category 3 business functions are in the low-risk group with a multiplier of .4.
3. For items A through E, determine the risk assessment factor for each business function or N/A.
4. For each business function, multiply the highest item number by the multiplier to obtain the risk rating for that business function.

Business Function	Rating	Risk Group/ Multiplier	Item A	Item B	Item C	Item D	Item E	Risk Rating
Pay vendor invoices								
Provide SPIR reporting data								
Participant Tracking								

Identification and sources of information

Name of State/SDA _____

Name/title of completer _____

Name/title of reviewer _____

Phone/E-mail for above _____

Date completed _____